Security Analysis Document

SA

Security Analysis Document

Version: 1.0
Date: 07/08/2014
Prepared by: Eduonix

Document History and Distribution

1. Version History

Version #	Date	Description	Author
V1.0	07/08/2014	First draft	Eduonix

2. Distribution

Recipient Name	Organisation	Distribution Method
Eduonix clients	Many	FTP

CONTENTS

1. INTRODUCTION 1
2. TEST ITEMS 2
3. APPROACH 2
4. ENVIRONMENTAL REQUIREMENTS 2
10. REPORT APPROVALS 3

1. INTRODUCTION

The Security Analysis document is designed to give as much information as possible to the bearer, about possible vulnerabilities and security risks in their system. It does not constitute 100% coverage, as a system can never be totally secure.

1.1 Objectives

To fully evaluate the Eduonix backup solution, to show any discovered security vulnerabilities. These issues will only be highlighted to senior management.

1.2 Testing Strategy

Purpose for this level of test,

- *Items to be tested – Eduonix backup solution*
- *Features to be tested - Vulnerabilities*
- *Features not to be tested – Systems outside of the backup environment*
- *Management and technical approach – Managed internally by QA, all tests conducted by Eduonix*
- *Pass / Fail criteria, - Information only – High, Medium & Low severities*
- *Individual roles and responsibilities – Management by Michael Knight, Tester Richard Martin*
- *Milestones - "Backup VA"*
- *Schedules – Tests to commence 08/08/2014 for 7 days*
- *Risk assumptions and constraints.*

1.3 Scope

Scope items;

Eduonix Backup Solution UI
Eduonix Backup Solution Server 172.16.50.2

2. TEST ITEMS

- *Test plan*
- *VA plan*
- *VA execution*

3. APPROACH

*v*ulnerability analysis consists of several steps:

- Defining and classifying network or system resources
- Assigning relative levels of importance to the resources
- Identifying potential threats to each resource
- Developing a strategy to deal with the most serious potential problems first
- Defining and implementing ways to minimize the consequences if an attack occurs.

If security holes are found as a result of vulnerability analysis, a vulnerability disclosure may be required. The person or organization that discovers the vulnerability, or a responsible industry body such as the Computer Emergency Readiness Team (CERT), may make the disclosure. If the vulnerability is not classified as a high level threat, the vendor may be given a certain amount of time to fix the problem before the vulnerability is disclosed publicly.

The third stage of vulnerability analysis (identifying potential threats) is sometimes performed by a white had using ethical hacking techniques. Using this method to assess vulnerabilities, security experts deliberately probe a network or system to discover its weaknesses. This process provides guidelines for the development of countermeasures to prevent a genuine attack.

3.1 Resources

1 Tester for duration
1 Test manager for duration
No exceptional equipment required

3.2 Schedule

Pending completion of tests, schedule is due to end on 13/08/2014, starting on 08/08/2014

4. ENVIRONMENTAL REQUIREMENTS

(Test environment must be segregated from any live system, because of the nature of the tests they may be intrusive and cause network disruption without warning. Therefore we

cannot guarantee uptime of any service in the same environment during this time.

4.1 Hardware

Rasperry Pi – Acting as proxy

4.2 Software

Kali
Metasploit
Nessus

4.3 Security

Security will be performed in isolation, requires metasploit framework community edition.

4.5 Publications

Software test plan
Software test coverage report
Software Pentest report
Software test case raw data

4.6 Risks and Assumptions

Due to storage requirements, the maximum backup we can test is 100GB, it is likely that backups will far exceed this in the field.

5. RESULTS & RECCOMMENDATIONS

Finding	Low	Medium	High	Comments

There are three areas that need to be addressed as a result of the internal scan:
system hardening, patch management, and user account management. Each one of these areas

should be first addressed at the Corporate Security Policy. Before procedures can be defined to address the corporate security policies, high-level solutions will be defined that address each of the three findings. Solution sets will then be listed and mapped to each finding area.

Approved by _____ Date__/__/____